

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	14	bahl.in. and "713"/\$.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 09:30
L2	4297	(705/26,27,37.ccls. 713/150-194.ccls.) and (invit\$ offer) and encrypt\$	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 09:31
L5	566	(705/26,27,37.ccls. 713/157,160.ccls.) and ((invit\$ offer) same access) and encrypt\$	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 09:34
S2	1	"20050044412".pn.	US-PGPUB	OR	ON	2007/06/29 15:04
S3	1	"6873977".pn.	US-PGPUB; USPAT	OR	ON	2007/07/06 15:30
S4	1	(non adj repudiable) adj certificate	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/06 15:31
S5	47	(repud\$) adj certificate	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/08 08:31


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Published before July 2004

Terms used: couriers encrypt messageFound **44** of **157,895**Sort results
by
Display
results
[Save results to a Binder](#)[Search Tips](#)
☐ Open results in a new
window
[Try an Advanced Search](#)[Try this search in The ACM Guide](#)

Results 1 - 20 of 44

Result page: [1](#) [2](#) [3](#) [next](#)Relevance scale ☐ ☐ ☐ ☐ ☐

1 [A method for obtaining digital signatures and public-key cryptosystems](#)



R. L. Rivest, A. Shamir, L. Adleman

February 1978 **Communications of the ACM**, Volume 21 Issue 2**Publisher:** ACM PressFull text available: [pdf\(748.63 KB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences: (1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key. (2) A message can be "signed" ...

Keywords: authentication, cryptography, digital signatures, electronic funds transfer, electronic mail, factorization, message-passing, prime number, privacy, public-key cryptosystems, security

2 [Cryptography and data security](#)



Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.Full text available: [pdf\(19.47 MB\)](#)Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

3 [Secure audit logs to support computer forensics](#)





Bruce Schneier, John Kelsey

May 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2
Issue 2

Publisher: ACM Press

Full text available: pdf(125.50 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

In many real-world applications, sensitive information must be kept in log files on an untrusted machine. In the event that an attacker captures this machine, we would like to guarantee that he will gain little or no information from the log files and to limit his ability to corrupt the log files. We describe a computationally cheap method for making all log entries generated prior to the logging machine's compromise impossible for the attacker to read, and also impossible to modify or delete ...

Keywords: audit logs, auditing, authentication, computer forensics, hash chains, intrusion detection

4 [Data Security](#)



Dorothy E. Denning, Peter J. Denning

September 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 3

Publisher: ACM Press

Full text available: pdf(1.97 MB)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

5 [A method for obtaining digital signatures and public-key cryptosystems](#)



R. L. Rivest, A. Shamir, L. Adleman

January 1983 **Communications of the ACM**, Volume 26 Issue 1

Publisher: ACM Press

Full text available: pdf(493.34 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences: Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key. A method ...

Keywords: authentication, cryptography, digital signatures, electronic funds transfer, electronic mail, factorization, message-passing, prime number, privacy, public-key cryptosystems, security

6 [Designing a global name service](#)



Butler W. Lampson

November 1986 **Proceedings of the fifth annual ACM symposium on Principles of distributed computing PODC '86**

Publisher: ACM Press

Full text available: pdf(760.57 KB)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

7 [Symmetric and Asymmetric Encryption](#)



Gustavus J. Simmons

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Publisher: ACM Press

Full text available:  pdf(2.23 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

8 Miscellany: Quantum cryptography in practice



Chip Elliott, David Pearson, Gregory Troxel

August 2003 **Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '03**

Publisher: ACM Press

Full text available:  pdf(809.93 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

BBN, Harvard, and Boston University are building the DARPA Quantum Network, the world's first network that delivers end-to-end network security via high-speed Quantum Key Distribution, and testing that Network against sophisticated eavesdropping attacks. The first network link has been up and steadily operational in our laboratory since December 2002. It provides a Virtual Private Network between private enclaves, with user traffic protected by a weak-coherent implementation of quantum cryptogra ...

Keywords: IPsec, cryptographic protocols, error correction, key agreement protocols, privacy amplification, quantum cryptography, quantum key distribution, secure networks

9 Authentication, confidentiality, and integrity extensions to the XNS protocol suite



R. Housley

October 1989 **ACM SIGSAC Review**, Volume 7 Issue 3

Publisher: ACM Press

Full text available:  pdf(462.79 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The Xerox Network Systems (XNS) architecture[1] includes all of the security features found in today's most popular protocol suites. In addition, XNS provides strong authentication at the beginning of each conversation. Authentication is the verification that both entities in a conversation are the ones claimed.[2] The Authentication Protocol [3] provides authentication in such a way that no passwords are ever transmitted on the network.

10 Secure communications over insecure channels



Ralph C. Merkle

April 1978 **Communications of the ACM**, Volume 21 Issue 4

Publisher: ACM Press

Full text available:  pdf(597.27 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

According to traditional conceptions of cryptographic security, it is necessary to transmit a key, by secret means, before encrypted messages can be sent securely. This paper shows that it is possible to select a key over open communications channels in such a fashion that communications security can be maintained. A method is described which forces any enemy to expend an amount of work which increases as the square of the work required of the two communicants to select the key. The method ...

Keywords: communications security, computer network security, cryptography, cryptology, key distribution, passive eavesdropping, public key cryptosystem, security, wiretap

11 Security issues on the internet



Carl Stephen Guynes, Richard G. Vedder, Michael T. Vanecek

 April 1997 **ACM SIGSAC Review**, Volume 15 Issue 2
Publisher: ACM Press

Full text available:  pdf(380.62 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The Internet is a collection of networks originally paid for by the U.S. Department of Defense. Its purpose was to provide a communications infrastructure more resilient to attack than the public communications channels in the event of war. When research became a priority in the 1960s and 1970s, money was given to the National Science Foundation, which became the de facto administrator of the network. The NSF ran the primary arteries of the Internet until the late 1980s. A substantial amount of ...


12 [Enabling crypto: how radical innovations occur](#)

 Arnd Weber
 April 2002 **Communications of the ACM**, Volume 45 Issue 4
Publisher: ACM Press

Full text available:  pdf(197.13 KB)  html(30.18 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Examining the key factors and influences in the development of cryptography.

13 [Security Mechanisms in High-Level Network Protocols](#)

 Victor L. Voydock, Stephen T. Kent
 June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2
Publisher: ACM Press

Full text available:  pdf(3.23 MB) Additional Information: [full citation](#), [references](#), [citations](#)

14 [The Satchel system architecture: mobile access to documents and services](#)

Mike Flynn, David Pendlebury, Chris Jones, Marge Eldridge, Mik Lamming
 December 2000 **Mobile Networks and Applications**, Volume 5 Issue 4

Publisher: Kluwer Academic Publishers

Full text available:  pdf(207.51 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Mobile professionals require access to documents and document‐related services, such as printing, wherever they may be. They may also wish to give documents to colleagues electronically, as easily as with paper, face‐to‐face, and with similar security characteristics. The Satchel system provides such capabilities in the form of a mobile browser, implemented on a device that professional people would be likely to carry anyway, such as a pager or mobile phone. Printing may be per ...


15 [Server-assisted cryptography](#)

 Donald Beaver
 January 1998 **Proceedings of the 1998 workshop on New security paradigms NSPW '98**

Publisher: ACM Press

Full text available:  pdf(1.13 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

16 [Responses to NIST's proposal](#)

 Ronald L. Rivest, Martin E. Hellman, John C. Anderson, John W. Lyons
 July 1992 **Communications of the ACM**, Volume 35 Issue 7

Publisher: ACM Press

Full text available:  pdf(8.06 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

17 [Dynamic analysis of security protocols](#)



Alec Yasinsac

February 2001 **Proceedings of the 2000 workshop on New security paradigms NSPW '00**

Publisher: ACM Press

Full text available:  pdf(871.04 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

18 [Distributed systems - programming and management: On remote procedure call](#)



Patrícia Gomes Soares

November 1992 **Proceedings of the 1992 conference of the Centre for Advanced Studies on Collaborative research - Volume 2 CASCON '92**

Publisher: IBM Press

Full text available:  pdf(4.52 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

The Remote Procedure Call (RPC) paradigm is reviewed. The concept is described, along with the backbone structure of the mechanisms that support it. An overview of works in supporting these mechanisms is discussed. Extensions to the paradigm that have been proposed to enlarge its suitability, are studied. The main contributions of this paper are a standard view and classification of RPC mechanisms according to different perspectives, and a snapshot of the paradigm in use today and of goals for t ...


19 [Macintosh human interface guidelines](#)



Apple Computer, Inc.

January 1992 Book

Publisher: Addison-Wesley Publishing Company

Full text available:  pdf(37.61 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Macintosh Human Interface Guidelines describes the way to create products that optimize the interaction between people and Macintosh computers. It explains the whys and hows of the Macintosh interface in general terms and specific details.

Macintosh Human Interface Guidelines helps you link the philosophy behind the Macintosh interface to the actual implementation of interface elements. Examples from a wide range of Macintosh products show good human interface design, including individ ...

20 [Implementing remote procedure calls](#)



Andrew D. Birrell, Bruce Jay Nelson

February 1984 **ACM Transactions on Computer Systems (TOCS)**, Volume 2 Issue 1

Publisher: ACM Press

Full text available:  pdf(1.56 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: distributed naming and binding, inter-process communication, performance of communication protocols, remote procedural calls, transport layer protocols

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)

IEEE Xplore[®]
RELEASE 2.3

Home | Login | Logout | Access Information | Alerts |

Welcome United States Patent and Trademark Office

BROWSE

SEARCH

IEEE XPLORE GUIDE

Search Results

Results for "(((couriers<in>metadata) <and> (encrypt<in>metadata))<and> (signed<..."

Your search matched 0 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

(((couriers<in>metadata) <and> (encrypt<in>metadata))<and> (signed<in>metad

Search

☐ Check to search only within this results set

Display Format: ☒ Citation ☐ Citation & Abstract

» Key

IEEE JNL

IEEE Journal or Magazine

IET JNL

IET Journal or Magazine

IEEE CNF

IEEE Conference Proceeding

IET CNF

IET Conference Proceeding

IEEE STD

IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

Help Contact Us Privacy & ;

© Copyright 2006 IEEE –

http://ieeexplore.ieee.org/search/searchresult.jsp?query1=couriers&scope1=metadata&op1=an... 7/8/07